DTMB Technology, Management & Budget	***State of Michigan Department of Technology, Management & Budget***	**TECHNICAL STANDARD**
Subject:	**Acceptable Use of State of Michigan (SOM) Information Technology (IT) Resources (former Ad Guide 1460.00)**	**Standard Number**
Authoritative Policy:	1340.00 Information Technology Information Security Policy	**1340.00.01**
Procedure Number:	TBD	
Distribution:	Statewide	

Purpose:

The purpose of this statewide standard is to identify acceptable use of state of Michigan (SOM) information technology (IT) resources and to provide awareness of expected end-user behavior. Unacceptable use of IT resources exposes the state to a number of unwarranted risks (*e.g.*, data breach, compromise or disruption of state network or application services) as well as other liability and legal issues.

Contact/Owner:

DTMB, Office of Michigan Cyber Security (MCS)

Scope:

Compliance with this standard is mandatory and its provisions apply to all authorized users who have been granted access rights to SOM IT resources.

Standard:

Acceptable uses of IT resources:

Technology resources are provided to employees and authorized representatives for the purpose of conducting official SOM business, state-sponsored activities, statutory and regulatory activities, use allowed by law, or other uses as authorized by agency business units, with the exception of behaviors identified as unacceptable in this standard.

State employees, volunteers, vendors, business partners, agents of local governments and other government agencies ("Users") may be authorized to access state IT resources to perform business functions with or on behalf of the state. They must be acting within the scope of their employment or contractual relationship with the state and must agree to use these resources in an efficient, effective, responsible, professional, ethical and lawful manner; utilizing approved applications, tools and mechanisms.

Users of SOM IT resources must adhere to this standard. Additionally, state employees are subject to the Civil Service Rules of Conduct. Users are expected to review these guidelines regularly. Failure to do so is not justification for non-compliance.

Issued: 4/3/2013
Revised:
Reviewed:
Next Review Date: 4/3/2014

Unacceptable uses of IT resources (include but not limited to):

Illegal Use

SOM IT resources may be used for lawful purposes only. Activity that is illegal under local, state or federal law; use that violates state or other applicable regulations, mandates, policies or standards; use that compromises public safety or the privacy of legally protected resident or citizen information; and activity that is malicious or fraudulent in nature is prohibited.

Users will abide by all copyright, trademarks, patent or other laws governing intellectual property. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without specific written permission of the copyright owner is not allowed.

Users shall respect and adhere to all licensing agreements and software license provisions. The installation of any software (including shareware and freeware) not authorized by DTMB for use on SOM computing devices is not allowed. No state-owned or licensed software may be installed, copied or used on non-state equipment unless explicitly approved by DTMB.

Abuse

Use of IT resources that takes away from or interferes with a user's work obligations or their conducting of authorized state business is not allowed.

IT resources shall not be used for commercial or personal product advertisements, solicitations, or promotions (including hosting of a personal web site); commercial or for-profit purposes; business or personal profit; political fundraising or lobbying; promotion of a social, religious, or political cause; gambling activity, gaming or online shopping.

Users shall not misrepresent their relationship with the state; imply state endorsement of products or services of a non-state entity; give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the state unless part of their legitimate job duties. All users should recognize that their state e-mail address (*e.g.*, user@michigan.gov) associates them with the state. Further, when web access is accomplished using an Internet address or domain name registered to the state, they may be perceived by others as officially representing the state or its employees.

When indicating place of employment as "State of Michigan" on personal (social media) web sites, or whenever expressing any personal opinion that may be mistaken for state policy, users shall add a disclaimer to any such communication. An example of disclaimer: "The opinions expressed here are my own and do not represent official policy of the state of Michigan".

Use of IT resources to access, display, process, perform, send, receive, or store any materials or content that is obscene, pornographic, lewd, lascivious, considered (categorized as) adult content, offensive, or excessively violent is prohibited. As is use of profanity, obscenity, racial terms, discriminatory remarks, or other language that may be offensive to another user; sending of hate mail or chain letters; harassment and other antisocial behaviors.

The state's network may not be used for downloading entertainment-type software or other files not related to the mission and objectives of the state for transfer to a user's home computer, personal device, or other media.

Security

Users are responsible for maintaining the security of sensitive or protected information. Providing to or sharing with unauthorized persons any information that is sensitive or protected by law, rule or regulation; posting of state information to external newsgroups, bulletin boards, or other public forums without authority; giving out personal information about another person unless part of legitimate job duties; storing of state information in public storage services unless approved by DTMB is prohibited.

Users are responsible for the reasonable protection and use of access granted to them and must follow all applicable security rules, policies and standards. Users shall not reveal their password to others or allow use of their account by others – this includes family and other household members when work is being done at home. Nor shall they leave workstations or other SOM resource (*e.g.*, laptop, smartphone, iPad) unattended without engaging password protections for the keyboard or device.

Users are responsible for the reasonable physical security and protection of state IT resources and devices physically in their possession.

Users shall not:

- Interfere with the normal operation of any IT resource.
- Act to disrupt systems or cause unnecessary network congestion or application delays.
- Intentionally attempt to compromise state systems or data.
- Cause intentional damage to or loss of data.

- Intentionally exploit vulnerability.
- Modify networks to circumvent security monitoring or access controls.
- Use tools or utilities to scan, probe, or attack a network.
- Intentionally re-route network traffic.
- Intercept or attempt to intercept data transmissions of any kind to which they are not authorized.
- Use unauthorized peer-to-peer (P2P) networking or P2P file sharing software or services.
- Use unauthorized instant messaging or unauthorized Internet Relay Chat (IRC) applications or services.
- Forward state e-mail messages to personal e-mail accounts, because of the unacceptable risk associated with privacy, security and compliance.
- Use any remote control software, tools or services on any internal or external computers, devices or systems not specifically set up by DTMB using methods authorized by policy or standard.
- Store state data or information in public storage services unless approved by DTMB.
- Post state information to external newsgroups, bulletin boards or other public forums without authority.
- Send unsolicited e-mail messages, including junk mail or other advertising material to individuals who did not specifically request such material (spam).
- Install or attach any unauthorized equipment to a state resource (*e.g.*, state's voice or data networks) without approval of DTMB and the resource owner. Examples of equipment include, but are not limited to: wireless access points, modems, disk drives, external hard drives, networking devices, personally-owned computers or mobile devices.
- Intentionally modify, damage, or remove IT resources that are owned by the state without proper authorization from DTMB and/or the owner of the resource.
- Intentionally modify, disable, test, or circumvent any IT resource security controls without authorization.
- Intentionally causing or creating the perception of an information security incident.
- Circumvent user authentication or compromise the security of any host, network or account.
- Seek or enable unauthorized access to any computer system, application or service.
- Intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.
- Misrepresent other users on the network.
- Access or attempt to gain access to any computer account to which they are not authorized.

- Access or attempt to access any portions of the state's network to which they are not authorized.
- Participate in activities that promote computer crime or misuse, including, but not limited to, posting or disclosing of passwords, credit card or other account numbers, and system vulnerabilities.
- Attempt to circumvent this standard through use of anonymous proxies, software or hardware.
- Use software or web sites (often called anonymizers) that attempt to hide Internet activity for the purpose of evading enterprise monitoring.
- Use device or software cleaning utilities to delete, remove, cover-up, hamper, and/or camouflage information of evidentiary value in response to an investigation.

No Presumption of Privacy

Users should have no expectation of privacy concerning their use of SOM IT resources, including e-mail or instant messaging, state-provided computing equipment, the SOM Intranet, SOM provided access to the public Internet, or other state information systems, except where applicable law provides differently.

The SOM actively monitors network services and IT resources, including, but not limited to, real time monitoring. Communications are considered to be state property and may be examined by management for any reason, including, but not limited to, security and/or employee conduct. Any evidence of illegal activity discovered during monitoring or reviews will be provided to the proper law enforcement organizations.

In addition, electronic records may be subject to the Freedom of Information Act (FOIA) and, therefore, available for public distribution.

Inadvertent and/or Erroneous Use

Users inadvertently directed to a web site that violates laws, regulations, polices or this standard may claim erroneous use. Mistakes can occur when using IT resources without any employee intent to violate policy. A claim of this type is only substantiated by connection times measured in seconds, rather than minutes when found in network, system or application log audits done to verify or detect abuse. Report to supervisors or managers when un-intentional misuse occurs. Self-reporting is encouraged and may be done without consequence.

Responsibilities:

Agencies

Agencies are responsible for ensuring that their users read and understand this standard. They must develop a process for certifying and documenting user acceptance.

Users

Must read this document, understand the expectations and take personal responsibility for adhering to the provisions of this standard. Each user will be required to acknowledge receipt of this standard and any agency specific addendums. Users must report all information resource violations to either their supervisor, manager, director, human resources, or Michigan Cyber Security.

Agents, contract staff, vendors, and volunteers

Are required to adhere to this standard, acknowledge an awareness of this standard, however realizing the consequences of willful violation will be appropriate to their status.

Supervisors, managers, or directors

Make up the first line of accountability for staff compliance with this standard and shall require that all staff under their management read, and acknowledge the acceptable use agreement, and abide by the provisions of this standard.

Agency Human Resources

Shall support supervisors and managers as needed in the awareness and disciplinary enforcement of this standard.

DTMB Information Technology Staff

Shall report suspected violations to MCS when found in the normal course of system support activity and assist MCS with audits and enforcement actions when requested to do so.

Office of Michigan Cyber Security (MCS)

Shall receive and document reports of suspected abuse from any source and act as necessary on each reports. MCS shall plan and supervise periodic system and network audits to detect potential abuse and shall use these audits to identify and investigate non-compliance with the provisions of this standard. Report incidents of abuse to an agency Human Resources, and agency internal auditor, and where abuse may involve criminal activity to appropriate state of Michigan or other law enforcement officials. Assist in the collection and preservation of digital forensic evidence when requested by law enforcement officials.

Agency Business Units

Shall ensure that all aspects of the IT Acceptable Use standard are communicated to staff within their divisions and work groups.

DTMB Procurement, Contract Administrators and Project Managers

Shall ensure contract agreements obligate contractors to comply with all IT policies, standards, and procedures which may change from time to time, and which will be made available to contractors upon their request.

Effect:

The policy described in this section sets a minimum level of conformance that will be implemented across the SOM enterprise. Agency work rules should support this policy direction and provide departmental guidance on how violations will be handled. State agencies desiring to implement more restrictive policies regarding information technology resources may do so by coordinating with MCS prior to implementation.

All categories of employees must realize that misuse or abuse of IT resources may lead to department or agency investigation and initiation of legal or disciplinary actions. Be aware that computers or resources assigned to you may also be removed from your office/work area for analysis.

Violation of this standard may result in agency-administered discipline up to and including discharge. Criminal or civil action may be initiated in appropriate instances.

Definitions:

Agency - Executive Branch entities including agency, department, board, or commission.

Business Units - Supervised areas of related work responsibility as explicitly defined and delegated to them by Executive Branch agency directors, boards, or commissions of the SOM.

Chain Mail - Unauthorized non-government or non-business related e-mail to large groups, the SOM address book, or to unspecific destination addresses that suggest that the receiver should further disseminate the message.

DTMB - Department of Technology, Management & Budget.

Hacking - Gaining or trying to gain unauthorized access to systems and databases either internal or external to the SOM computer systems or networks for the purpose of viewing, stealing, or corrupting data.

IT systems or resources - Data, networks (over any media type); computer devices, including: servers, hosts, laptops, desktops, handheld, or tablet personal computer; communication devices: phone, web phones, or pagers; and software applications accessed with any interface.

MCS - DTMB Office of Michigan Cyber Security.

Resource - A person, asset, material, or capital which can be used to accomplish a goal.

SOM - State of Michigan.

SOM information technology resources - The IT systems and resources that the SOM uses for conducting state business.

Users - Includes the broad range of persons, including but not limit to, state employees (including interns), volunteers, vendors, business partners, agents of local governments and other government agencies, who have been granted access (given a password) to specific SOM IT resources, applications or data for the purpose of performing business functions with or on behalf of the state.

Approving Authority:

John E. Nixon, CPA
Director

Issued: 4/3/2013